فضای مجازی و اصول حقوق بین‌الملل حاکم بر آن با رویکرد حقوق رسانه ای

مصطفی زارعی [۱] ، مریم اسپرغم [۲] ،محمد چمکوری [۳]

تاریخ دریافت: ۱۸/ ۴/ ۱۳۹۷

تاریخ پذیرش: ۲۶/ ۷/ ۱۳۹۷

چکیده

حقوق بین الملل را حقوق حاکم بر روابط بین المللی می خوانند که از دیرباز مناسبات میان کنشگران بین المللی و خاصه دولت ها در خصوص حاکمیت بر سرزمین و منابع طبیعی آنها و یا قلمرو دریایی و هوایی آنان را مشخص می کرده است، رفته رفته، پیشرفت علوم و فنون باعث شده تا حقوق بین الملل علاوه بر فضای زمین و دریا و هوا به فضای جو و حتی ماورای جو نیز نظر افکند و قوانین و مقرراتی را برای ساماندهی به امور جاری در این مناطق نیز طراحی و جاری نماید. پدیده حاضر، مرز جدیدی میان دنیای سایبری و دنیای حقیقی به وجود آورده که تهدید بزرگی در مقوله فقدان قانون و همچنین عدم امکان اجرای تمام و کمال قانون احساس می شود. استفاده دولت ها از فضای ناامن سایبری، زمینه را برای بسیاری از هم نوعان خود جهت خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته اند. اقدام به قانون گذاری در برخی کشورها، بسته به میزان پیشرفت در دنیای فناوری، جامعه بین المللی را نیز به فکر واداشته که بتواند در این آشفته بازار فضای مجازی، اقدامی هرچند اندک به منظور تلطیف این فضا انجام دهد. نوشتار حاضر به دنبال پاسخگویی به این سوال کلیدی است که اصول و قواعد حقوق بین الملل حاکم بر فضای مجازی بعنوان رسانه ای نوین چیست و آیا اصول و وقواعد موجود توفیقی در تنظیم روابط دولت و سازمان های بین المللی در عرصه اینترنت داشته است.

واژه‌های کلیدی:

رسانه ،فضای مجازی، حقوق بین الملل

---

[۱]. دانشجوی دکتری حقوق بین الملل،مرکز تحصیلات تکمیلی دانشگاه پیام نور،تهران،ایران ، **Email:mostafakb86@gmail.com**

[۲] -کارشناس ارشد حقوق خصوصی و مدرس دانشگاه

[۳]. استادیار حقوق دانشگاه پیام نور،بوشهر،ایران

مقدمه و بیان مسئله

رسانه های نوین با در دست گرفتن افکار عمومی وکنترل و هدایت آن در سطح جهانی ،نقش جدیدی در عرضه سیاسی و اجتماعی بازی می کنند.به ویژه که امروزه،رسانه ها از نظر تعداد و کیفیت تنوع بسیاری پیدا کرده اند.اینترنت یکی از بانفوذترین تکنولوژی جدید ارتباطی است که همه ابعاد زندگی بشر را تحت تاثیر عظمت نفوذ خود قرار داده است.

بواسطه محبویت روزافزون و رشد کمی و کیفی این رسانه به نظر می رسد دیگر نمی توان چشمها را بر روی تاثیرات اجتماعی و سیاسی ،حقوقی و...در عرصه ملی و بین المللی آنها فرو بست. (زارعی و همکاران،۱۳۹۵:۶۱)

روند رو به رشدی که فضای مجازی در دو دهه‌ی اخیر طی کرده نیاز به قانون گذاری در این حوزه را هر روز بیش از بیش می‌نماید. این امر به نوبه خود چه در سطح داخلی و چه در سطح بین‌المللی چالش‌هایی را به دنبال داشته است. برخی از این چالش‌ها با بهره‌گیری از اصول حقوق کنونی به راه حل‌هایی رسیده‌اند که از آن میان می‌توان به اختلافات بر سر صلاحیت قضایی میان کشورها تروریسم سایبری و جنگ سایبری حمایت از مالکیت معنوی در فضای سایبر و حمایت از حریم خصوصی در فضای سایبر و کنترل محتوا در مقابل آزادی بیان در اینترنت اشاره کرد، که در مواجهه با مسائلی از این دست حقوق بین‌الملل نقش کلیدی ایفا می‌کند. اما جامعه جهانی در این حیطه با چالش‌های جدیدی روبرو است که هنوز بر سر آن‌ها بحث و تبادل نظر در جریان است و راه حل قطعی حاصل نگردیده است اما شاید اعمال رژیم حقوقی میراث مشترک بشریت بر منابع اینترنت بتواند به عنوان راهکاری برای گذار از این مرحله کار آمد واقع شود. دسترسی به اینترنت به عنوان یکی از موضوعات حقوق بشر نیز یکی دیگر از موارد نو ظهور در این حیطه است، که باز هم حقوق بین‌الملل یکی از بازیگران اصلی در این خصوص به شمار می‌آید. پس از بررسی لزوم قانونمندسازی اینترنت و چالش‌های مربوط به آن ارائه چارچوبی مناسب برای دستیابی به فضای قانونمند مقتضی می‌نماید. در این راستا حقوق بین‌الملل به واسطه‌ی ویژگی‌های منحصر به فرد خود بیشترین تناسب را برای قانون‌گذاری در این حیطه داراست. به نظر می‌رسد در میان تمام مدل‌هایی که توسط صاحب‌نظران به عنوان چارچوبی برای قاعده‌مند کردن این حوزه ارائه شده و تا رسیدن به یک الگوی جامع و هماهنگ بر اساس حصول توافقات جدید میان تمام کشورها، مدل قانون‌مند کردن اینترنت در چارچوب سازمان ملل به دلیل تناسبی که با خواست‌ها و ویژگی‌های اینترنت دارد، مقتضی‌ترین الگو بشمار می‌رود.(تحریری،۱۳۸۹:۹۳).

در این پژوهش مابه دنبال یافتن پاسخی پیرامون این سوالات کلیدی هستیم که اصول حقوق بین الملل حاکم بر فضای مجازی به عنوان رسانه ای که اکنون تبدیل به رسانه ای جهانی شده است چیست؟ واکنش‌های حقوقی دولت‌ها و سازمان‌های بین‌المللی به جرایم سایبری چه بوده است؟و اینکه دولت ها در قالب معاهدات و توافق نامه های بین المللی و همچنین سازمان های بین المللی دولتی و غیر دولتی تا چه در به نظم کشیدن این رسانه در عرصه های ملی و بین المللی موفق بوده اند؟

۱۱-اصول حقوق بین الملل حاکم برفضای مجازی

اصول حاکم بر اینترنت از چند جهت حائز اهمیت هستند. اولا اینکه برای آشنایی بیشتر با این محیط می توان به سراغ این اصول رفت و با توجه به آنها شناخت بیشتری را از واقعیت های محیط وب بدست آورد. از سوی دیگر شناخت آنها می تواند تاثیر بسزایی در قانونگذاری و ایجاد قواعد حقوقی داشته باشد چرا که برای صحت و سلامت یک قانونگذاری یکی از اصولی ترین قدم ها شناخت اصول حاکم بر پدیده است، به همین دلیل مهمترین این اصول را ذکر می کنیم.

۱-۱ اصل آزادی دسترسی به اطلاعات

عده ای از کارشناسان تلاش فراوانی به خرج می دهند تا از نفوذ دولتها به عرصه ی مدیریت اینترنت جلوگیری کنند؛ ولی حتی اگر در این راه موفق نباشند مطمئناً نخواهند گذاشت اصل آزادی دسترسی به اطلاعات مورد خدشه واقع گردد .البته این

اصل با یکسری چالش هایی مواجه است. برای مثال آمار و ارقام درباره ی کاربران اروپایی و آمریکایی اینترنت در مقایسه با کاربران آفریقایی، وضعیت وحشتناکی را به نمایش می گذارد. از سوی دیگر و از آنجا که قریب به ۷۰ درصد اینترنت با زبان انگلیسی نگاشته شده است می توان تصور کرد که تا چه اندازه متکلمان به سایر زبان ها توان استفاده از آنرا خواهند داشت. با همه ی این احوال و با همه ی اعتراضاتی که مبدعان و مدیران اینترنت به این امر داشته اند لیکن تلاش جهانی بر این است تا اصل آزادی دسترسی به اطلاعات همچنان بی خدشه باقی بماند.

۲-۱اصل تخصصی بودن اداره ی اینترنت

دانشمندان معتقدند اصولا دولتها قادر به اداره ی اینترنت نیستند؛ زیرا این مسئله یک امر کاملا تخصصی است. از همین رو دولتها، [۴] ITUرا برای قائم مقامی برگزیده اند. اتحادیه ی بین المللی مخابرات، یک نهاد تخصصی سازمان ملل است و وظایف آن بیشتر از همه، به حال و روز اینترنت می آید.

۳-۱ همیشه در دسترس بودن و پاسخگویی به همه

اینترنت به شکلی طراحی شده است که امکان تعطیلی برای آن وجود نداشته باشد. علاوه بر آن، امکانات لازم برای دستیابی به اینترنت برای همه ی مردم به صورت یکسان وجود داشته و به عبارتی، سهل الوصول ترین راه برای دستیابی به اطلاعات به شمار می رود. این اصل نتیجه ی عملی اصل اول یعنی آزادی دسترسی به اطلاعات به شمار می آید.

۴-۱اصل تمرکز زدایی و عدم امکان اخراج

تمرکز زدایی در محیط سایبر به این معناست که هیچکس نمی تواند با به تعطیلی کشاندن یک کامپیوتر خاص، اینترنت جهانی را خاموش کند. طراحان اینترنت سعی کرده اند اوضاع به شکلی پیش رود که اگر یک قسمت از مراکز مدیریت اینترنت خراب شد مراکز دیگر وظایف آنرا به عهده بگیرند. این مسئله بر امکان دوام شبکه می افزاید. مسئله ی بعد، عدم امکان اخراج هیچ کاربر توسط هیچ مرجع موجود می باشد. یعنی تا هر وقت، هر فرد با هر عقیده ای می تواند در محیط اینترنت باقی بماند و علاوه بر کسب اطلاعات و دانایی به بسط و گسترش عقاید خویش بپردازد. این امکان که یک پلیس در شبکه وجود داشته باشد هر چند به راحتی می تواند فراهم گردد لیکن با اصل عدم امکان اخراج، سازگاری ندارد. بسیاری از اطاق های گفتگو برای رعایت اصول خود، به این راه حل متوسل می شوند؛ لیکن اصل اساسی در اینترنت، عدم توسل به چنین حربه ای است.

شاید نتوان گفت که تمامی اصول حاکم بر وب در همین اصول قرار دارد لیکن آنچه حائز اهمیت به نظر رسیده در این اصول جمع آوری گردیده است.

۲.چالشهای پیشگیری از جرائم فضای مجازی با موازین حقوق بشر

گرچه فضای سایبر این پدیده ی شگفت‌انگیز قرن بیست و یکم، بسیاری از عرصه‌ها را با تحولات بنیادین مواجه کرده؛ اما سوء استفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری در این زمینه شده است. با توجه به مشکلات بسیاری که فراروی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب‌ترین تدبیر سیاست جنایی است. در این میان، پیشگیری وضعی یکی از اقدامات مهم محسوب می‌شود، اما با محدودیتهایی مواجه است که از جمله ی آنها نقض موازین حقوق بشر[۵] است. ماهیت

---

[۴] - ITU International Telecommunication Union:

اتحادیه بین‌المللی مخابرات یا آی تی یو **(ITU)**،یک سازمان بین‌المللی وابسته به سازمان ملل متحد است. این اتحادیه دومین اتحادیه قدیمی پس از کمیسیون راین است. این اتحادیه وظیفه قانون‌گذاری و مدیریت فضای فرکانسی، تدوین استانداردهای تبادل داده و اطلاعات و همچنین کمک به رشد و توسعه ارتباطات در سراسر جهان را بر عهده دارد. مقر این سازمان در ژنو سوئیس است.

[5] - Human rights standards

فضای سایبر به گونه‌ای است که تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را موجب شده و همچنین با امکاناتی که جهت برقراری انواع ارتباطات ایمن فراهم آورده، به نوعی در جهت حفظ حریم خصوصی افراد گام برداشته است؛ اما تدابیر پیشگیرانه ی وضعی از جرائم سایبر، عمدتاً به گونه‌ای اجرا می‌شوند که این سه اصل حقوق بشری را نقض می‌کنند. کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند (صفاری، ۱۳۸۰: ۲۹۲)

در این زمینه، شیوه‌های مختلفی از سوی جرم‌شناسان ارائه شده که از مهمترین آنها می‌توان به شیوه‌های دوازده‌گانه ی کلارک[6]، جرم‌شناس انگلیسی، اشاره کرد که آنها را در سه گروه چهارتایی قرار داده است:

الف) دشوار ساختن ارتکاب جرم از طریق: الف. حفاظت از آماجها و قربانیان جرم؛ ب.کنترل و ایجاد محدودیت در دسترسی به موقعیتهای جرم‌زا؛ ج. منحرف کردن مجرمان؛ و د. برچیدن ابزار ارتکاب جرم.

ب) افزایش خطرپذیری مجرمان از طریق: الف. مراقبت از ورودیها و خروجیها؛ ب. مراقبت رسمی؛ ج. مراقبت غیررسمی؛ و د. مراقبت طبیعی.

ج) کاهش جاذبه از آماجها و قربانیان جرم از طریق: الف. حذف آماجهای جرم؛ ب.علامت‌گذاری اموال؛ ج. تقلیل فرصتهای وسوسه‌انگیز؛ و د. وضع قواعد خاص (ابراهیمی، ۱۳۸۳: ۱۸).

بدیهی است بحث راجع به هر یک از این شیوه‌ها خود مجال دیگری می‌طلبد و در اینجا فقط برای آشنایی با این حوزه و همچنین تطبیق آنها با شیوه‌هایی که نسبت به جرائم سایبر به اجرا درمی‌آیند، به آنها اشاره شد.

آنچه در این قسمت مورد بررسی قرار می‌گیرد، تدابیر پیشگیری وضعی از جرائم سایبر و چالش آنها با رعایت موازین حقوق بشر است.

۱-۲ تقابل پیشگیری وضعی از جرائم رایانه‌ای با آزادی بیان و جریان آزاد اطلاعات

از آنجا که این دو اصل از لحاظ ماهیت تقریبا مشابه یکدیگرند و حتی می‌توان آنها را لازم و ملزوم یکدیگر برشمرد و چون تدابیر پیشگیرانه از جرائم سایبر به یک شکل به آنها تعرض می‌کنند، در اینجا با یکدیگر بررسی خواهند شد.

ماهیت آزادی بیان به گونه‌ای است که باید دیدگاهها و عقاید افراد بدون محدودیت در اختیار همگان قرار گیرد. این مبنا کاملاً با آنچه فضای سایبر فراهم می‌آورد منطبق است و حتی زمینه‌های شکوفایی آن به مراتب فراتر از آنچه تصور می‌رفت به وجود آمده است. از سوی دیگر، تدابیر محدودکننده یا سلب‌کننده ی دسترسی، به ویژه فیلترینگ، مانع بزرگی در تحقق این اصل محسوب می‌شوند، زیرا از جریان آزاد اطلاعات جلوگیری می‌کنند. دلایل مختلفی باعث ایجاد محدودیت از سوی این ابزارها می‌شود که در اینجا به دو عامل مهم اشاره می‌شود:

الف. مراجع تدوین‌کننده ی فهرستها :معمولاً کسانی مبادرت به تدوین فهرست فیلترها می‌کنند که درباره ی برخی موضوعات مانند مسائل مذهبی، اخلاقی یا سیاسی تعصب دارند و می‌کوشند از دسترسی دیگران به سایتهایی که مغایر با اعتقاداتشان است جلوگیری کنند. اما آنچه بیشتر به گستره ی اعمال این محدودیتها دامن می‌زند، گنجاندن طیف وسیعی از موضوعات مشکوک یا به اصطلاح خاکستری در فهرستهای سیاه است. مراجع مذکور این کار را برای تحقق هرچه بیشتر اهدافشان انجام می‌دهند، فارغ از اینکه این اقدام تا چه حد می‌تواند از دسترسی افراد به مطالب معتبر و مجاز جلوگیری نماید.

ب. کارکرد انطباقی :دومین مانع بزرگ، کارکرد انطباقی و نه هوشمندانه ی این ابزارهاست. همانطور که می‌دانیم، اصطلاحات یا تصاویر مندرج در فهرستهای سیاه، تنها در متون یا محتواهای غیرمجاز به کار نمی‌روند و بسیار اتفاق می‌افتد که به لحاظ کاربرد آنها در محتواهای مجاز، از دسترسی به آنها جلوگیری می‌شود. به عنوان مثال، با درج واژه ای خاص در موتورهای

---

[6] - Clarke

جستجو که در مجامع عمومی شرم به زبان راندن آن واژه وجود دارد، فیلترها به سرعت فعال می‌شوند، در حالی که بسیار اتفاق می‌افتد که از آن واژه در متون معتبر علمی و ادبی نیز استفاده می شود(Thornbburgh, 2004: 267).

امروزه در بسیاری از کشورها حفظ امنیت ملی، نظم، سلامت یا اخلاق عمومی و احترام به حقوق یا آزادیهای اساسی دیگران، جزء مولفه‌هایی است که به رسمیت شناخته شده و دولتها تلاش می‌کنند از آنها به بهترین وجه پاسداری کنند. از سوی دیگر، فضای سایبر جلوه ی دیگری به این مفاهیم بخشیده و باید مطابق با ویژگیهای خاص آن برنامه‌ریزی کرد. اگر تعداد بسیار کمی از گروههای یک جامعه به فکر تهیه ی انواع ابزارهای محدودکننده یا سلب‌کننده ی دسترسی هستند، خیل عظیمی هم برای خنثی کردن آن ابزارها تلاش می‌کنند و در میان این گروه می‌توان چهره‌های موجه بسیاری نظیر دانشجویان و دانش‌پژوهان را یافت که برای احقاق حق خود، یعنی بهره‌برداری علمی و سودمند از این فضا، سعی می‌کنند دست به کاری بزنند که شاید غیرقانونی نیز تلقی شود.

آنچه نباید از نظر دور داشت اینکه در تمامی کشورها، حتی آنهایی که خود را مهد مردم‌سالاری می‌دانند، خط قرمزهایی وجود دارد. در کشوری مثل ایالات متحده یا کشورهای اروپایی، از ابزارهایی نظیر فیلترها به وفور استفاده می‌شود، اما برای کاستن از مضرات آنها، سعی شده برنامه‌ریزی مفصلی در زمینه ی مخاطب‌شناسی (کسانی که این ابزارها برای آنها به کار می‌رود)، شناسایی هرچه دقیقتر محتواهای غیرمجاز و پرهیز از گنجاندن موارد مشکوک به آنها و در نهایت بهره‌گیری چندبعدی از این ابزارها انجام شود. به عنوان مثال، در کنار فهرستهای متنی، از فهرستهای تصویری یا دیگر شناسه‌ها استفاده می‌شود تا ضعف این ابزارها به حداقل برسد.

به نظر می‌رسد با یک برنامه‌ریزی صحیح و اقتباس از الگوهای مفیدی که اکنون در دیگر کشورها به اجرا درمی‌آید، علاوه بر حفظ ارزشهای مورد قبول جامعه، می‌توان به گونه‌ای موثر از جرائم سایبر پیشگیری کرد.

۲-۲ تقابل پیشگیری وضعی از جرائم رایانه‌ای با حریم خصوصی

همانگونه که اشاره شد، فضای سایبر برخلاف اصول گذشته، زمینه‌های تهدید و تعرض به این اصل را بیشتر کرده است. از آنجا که این اصل به حریم و خلوت افراد مربوط می‌شود، نسبت به دیگر اصول بیشتر مورد توجه قرار گرفته و در این زمینه قوانین و مقررات سخت و لازم‌الاجرایی به تصویب رسیده که آنها را به اجمال بررسی خواهیم کرد.

اما پیش از پرداختن به قوانین و مقررات حمایتی از حریم آنلاین افراد، به تاثیر ابزارهای پیشگیرانه از جرائم سایبر آن اشاره می‌شود.

به طور کلی، دو ابزار پیشگیرانه، حریم الکترونیکی افراد را تهدید می‌کنند: اولین ابزار در این زمینه، ابزارهای نظارتی است که تردیدی در تعرض‌آمیز بودن آنها نیست. چنانچه در محیطی این حس در مردم بیدار شود که به دلیل بی‌اعتمادی به آنها، همواره تحت نظارت قرار دارند، این امر به شدت در نحوه ی فعالیت آنها تاثیر خواهد گذاشت. این خود به معنای ناکام ماندن اهدافی است که از ظهور این فضا دنبال می‌شد. به هر حال، با اذعان به اینکه ضروری است برای مقابله با جرائم بسیار متنوع سایبر اقدامات نظارتی اعمال شود، این نظارت باید به نحوی باشد که اعضای این فضا احساس نکنند به آنها به دید مجرم نگریسته می‌شود.

دومین ابزاری که البته به صورت غیرمستقیم حریم افراد را تهدید می‌کند، سیستمهای تائید هویت است. در فضای سایبر، برای اینکه به اشخاص اجازه ی ورود به محیطهای خاصی داده شود، برخی اطلاعات که شامل اطلاعات شخصی یا حتی اطلاعات شخصی حساس می‌شود، از آنها اخذ می‌گردد. نگرانی که در اینجا وجود دارد، راجع به امکان سوء استفاده ی متصدیان این سایتها از این اطلاعات یا امکان افشای آنها به دلایل مختلف است(Kent, 2004: 55).

اما راجع به اسناد بین‌المللی و منطقه‌ای درباره ی حمایت از این اصل، ابتدا باید به ماده ی ۱۵ کنوانسیون جرائم سایبر۲۰۰۱بوداپست[۷]، اشاره کرد که با رویکردی عام از دول عضو خواسته است قوانین و مقررات خود را برای حمایت از حقوق و آزادی های بشر که در کنوانسیون شورای اروپا[۸]، میثاق بین‌المللی حقوق مدنی و سیاسی[۹] و دیگر اسناد لازم‌الاجرای بین‌المللی منعکس شده تصویب کنند و به اجرا درآورند. این، حاکی از توجه کامل واصفان این کنوانسیون به رعایت موازین حقوق بشر در فضای سایبر است. همچنین می‌توان به اسناد ۳۱۳/۹۰/ EECو 2001/29/ECشورای اروپا راجع به قواعد جامعه ی اطلاعاتی اشاره کرد.

در حوزه ی حریم خصوصی، مراجع قانونگذاری اروپا پیش از این دستورالعملهای مختلفی برای حمایت از حریم الکترونیکی اشخاص به تصویب رسانده‌اند که به طور فهرست‌وار به آنها اشاره می‌گردد: ۱. کنوانسیون شورای اروپا راجع به حمایت از اشخاص در برابر پردازش خودکار اطلاعات شخصی (۱۹۸۱) ؛ ۲ .دستورالعمل اتحادیه ی اروپا راجع به حمایت از داده‌ها (۴۶/۹۵(EC/؛ ۳ .دستورالعمل مخابرات اتحادیه ی اروپا برای حمایت از پردازش داده‌های شخصی و حریم افراد در حوزه ی مخابرات که در آن، مباحث مربوط به شبکه‌های اطلاع‌رسانی رایانه‌ای را هم مطرح کرده است(۶۶/۹۷//EC؛) و ۴. دستورالعمل پارلمان و شورای اروپا در خصوص پردازش داده‌های شخصی و حمایت از حریم ارتباطات الکترونیک (۵۸/۲۰۰۲EC)

اما در ایالات متحده، اولین قانون فدرال حمایت از حریم ارتباطات الکترونیک، در سال ۱۹۸۶ به تصویب رسید. ویژگی بارز این قانون این بود که بر خلاف اصلاحیه ی چهارم قانون اساسی، تمامی افراد مرتبط با حوزه ی ارتباطات الکترونیک، به ویژه ارائه‌دهندگان خدمات شبکه‌ای را تحت شمول خود قرار داده و برای نقض حریم افراد از سوی آنان، ضمانت اجراهای کیفری و غیرکیفری مقرر کرده است. البته این قانون استثناهایی را در این زمینه برشمرده که از جمله آنها می‌توان به مجاز بودن ارائه‌دهندگان خدمات در نقض حریم افراد برای حفاظت از اموال، حقوق و دارایی هایشان اشاره کرد. همچنین قانون نحوه ی استفاده از ابزارهای ثبت‌کننده و ردیاب، راجع به نحوه ی شنود و نظارت مجریان قانون بر ارتباطات مخابراتی و الکترونیکی است(Usdoj, 2002: 4).

اما مهمترین نکته‌ای که باید راجع به قوانین مصوب در ایالات متحده به آن اشاره کرد، مواردی می باشد که این کشور پس از واقعه ی یازدهم سپتامبر در سال ۲۰۰۱ اعمال کرده است. کمتر از دو ماه از این واقعه نگذشته بود که قانون بسیار مفصلی تحت عنوان قانون پاتریوت[۱۰] برای مبارزه با تروریسم و حفظ امنیت ملی به تصویب رسید که به موجب آن تمامی قوانین گذشته ی

---

7 - Cyber Crime Convention 2001 Budapest**:**

کنوانسیون جرایم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» یا به اختصار «کنوانسیون بوداپست» نخستین معاهده بین‌المللی است که به جرائم رایانه‌ای و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کرده، روش‌های تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد. این کنوانسیون توسط شورای اروپا در سال ۲۰۰۱ ارائه شد و از ۲۳ نوامبر ۲۰۰۱ کشورها می‌توانستند آن را امضا کنند. از ابتدای جولای ۲۰۰۴ کنوانسیون به اجرا درآمد**.**

8 - Council of Europe Convention**:**

شورای اروپا **(Council of Europe**)،کهن‌ترین سازمان برای یکپارچه‌سازی اروپاست که در سال ۱۹۴۹میلادی دایر گشت. پایهٔ این سازمان بر گسترش مردم‌سالاری، حقوق بشر، زمامداری قانون و بهره‌برداری از همکاری‌های فرهنگی استوار است**.**

9 - International Covenant on Civil and Political Rights

۱۰ - لایحه میهن‌دوستی آمریکا **(USA PATRIOT Act)** ،بلافاصله بعد از حملات ۱۱ سپتامبر ۲۰۰۱ در کنگره آمریکا مطرح شد و با رای بسیار بالا به تصویب نمایندگان سنا و کنگره آمریکا رسید و بعد از امضای رئیس جمهور به قانون لازم‌الاجرا تبدیل شد. این قانون با الحاق مفاد متعددی به قوانین مربوط به مهاجرت و امنیت در واقع مقررات مربوط به اقامت، تابعیت و مهاجرت شهروندان غیرآمریکایی مقیم آمریکا را سخت می‌کند و به دستگاه مجریه اجازه می‌دهد که آزادانه‌تر از گذشته و به بهانه ضرورت امنیتی به اقدام پیشگیرانه در داخل آمریکا دست بزند.

حمایت از حقوق بشر اصلاح شد و به مجریان قانون و دیگر اشخاص دست اندرکار، نظیر متصدیان شبکه‌ها، اجازه داده شد به حریم اشخاص، به ویژه حریم آنلاین آنها تعرض کنند.(United Nations, 2004: 40) .

۳-واکنش های قانونی به فضای مجازی و جرایم مرتبط

پیشرفت فناوری های ارتباطی و اطلاعاتی و به تبع آن توسعه فضای مجازی با وجود دستاوردها و کارکردهای فوق‌العاده در زمینه‌های اجتماعی، فرهنگی، اقتصادی و سیاسی به آسیب‌ها و مشکلاتی نیز دامن زده است .سوء استفاده از این فضا برای جرم و بزهکاری، از آن جمله است. در مواجهه با این نوع از جرایم سایبری که گاه جنبه فراملی و بین المللی نیز به خود می‌گیرد، دولت‌ها و سازمان‌های بین‌المللی از دهه ۷۰ به بعد با تدوین و قوانین و قواعد حقوقی جدید به مبارزه برخواسته‌اند.

۳-۱ واکنش تقنینی کشورها در مورد جرائم سایبر

تا دهه ی ۱۹۷۰ میلادی کشورهای مختلف در چارچوب قوانین سنتی با جرائم سایبر برخورد می‌کردند؛ اما پیشرفت فناوری اطلاعات، تنوع و کثرت سوء استفاده‌هایی که از این فناوری به عمل آمد، حقوق جزای سنتی کشورها را به چالش کشید.

یکی از علل به چالش کشیده شدن حقوق جزای سنتی این بود که قوانین کیفری کشورها تا قبل از شیوع جرائم سایبری غالباً به حمایت از اهداف و موضوعات ملموس می‌پرداختند. با رشد فناوری رایانه، اطلاعات و داده‌های رایانه‌ای به عنوان یک موضوع غیرملموس، غیر قابل رؤیت و با ارزش، موضوع جرم سایبری قرار گرفت. حقوق جزای ماهوی که حمایت از ارزشها را بر عهده دارد در برابر تجاوز و تعدی به این ارزشها با نگرشی جدید واکنش نشان داد. این نگرش طی مراحلی موجب اصلاح سیستم‌های قضایی شد.

پروفسور زیبر آلمانی (پدر حقوق کیفری اطلاعات) به پنج مرحله از این مراحل به ترتیب زیر اشاره کرده است:

اولین مرحله، اصلاح سیستم‌های قضایی غرب بود، که در حمایت از محرمانگی (حقوق خصوصی و فردی) در دهه‌های ۱۹۷۰و۱۹۸۰ ظاهر شد. این تقنین، واکنشی در برابر چالش‌های جدید مربوط به حقوق خصوصی و فردی بود که به واسطه ی امکانات جمع‌آوری، ذخیره‌سازی و انتقال داده‌ها از طریق تکنولوژی جدید با مسائل جدید مواجه شده بود. لذا قوانینِ جدیدِ حمایت از داده‌ها، در حمایت از حقوق خصوصی و فردی شهروندان از جنبه ی اداری، مدنی و کیفری در کشورهای مختلف تصویب شد. قوانین کانادا و استرالیا در سال ۱۹۷۲، سوئد ۱۹۷۳، آمریکا ۱۹۷۴، آلمان۱۹۷۷، فرانسه، نروژ، اتریش و دانمارک ۱۹۸۸، ایسلند ۱۹۸۱، بریتانیا ۱۹۸۴، ایرلند، ژاپن و هلند ۱۹۸۸ تصویب شده‌اند و بعضاً این قوانین جدید مورد اصلاح قرار گرفته‌اند.

مرحله ی دوم از موج قوانین اصلاحی ناظر بر جرائم اقتصادی مرتبط با رایانه در اواخر دهه ی۱۹۷۰ و دهه ی ۱۹۸۰ است. آمریکا درسال ۱۹۷۶ (در سطح ایالات)، ایتالیا ۱۹۷۸، استرالیا ۱۹۷۹، بریتانیا۱۹۸۱، آمریکا۱۹۸۴ (درسطح فدرال)، دانمارک وکانادا ۱۹۸۵، آلمان۱۹۸۶، سوئد و شیلی۱۹۸۷، اتریش، ژاپن و نروژ ۱۹۸۷، فرانسه و یونان ۱۹۸۸، فنلاند و بریتانیا ۱۹۹۰ قوانینی در خصوص جرائم رایانه‌ای اقتصادی وضع کرده‌اند که بعضی از این قوانین چند بار اصلاح شده‌اند.

مرحله ی سوم قوانین اصلاحی در دهه ی ۱۹۸۰ ناظر بر جرائم مالکیت معنوی مرتبط با رایانه است. بعد از اینکه برنامه‌های رایانه‌ای در دهه ی ۱۹۷۰ تحت حمایت حق اختراع قرار گرفت، قوانین اصلاحی برنامه های رایانه‌ای را مشمول کپی رایت (مالکیت معنوی) قرار دادند. کشور آمریکا در سال ۱۹۸۰، مجارستان ۱۹۸۳، استرالیا، هند و مکزیک ۱۹۸۴، شیلی، آلمان، فرانسه، ژاپن و انگلستان در ۱۹۸۵، برزیل، کانادا و اسپانیا در ۱۹۸۸، دانمارک، کلمبیا و سوئد ۱۹۹۰ و نروژ در ۱۹۹۱ قوانین

مربوط به مالکیت معنوی (کپی رایت) خود را اصلاح کرده‌اند و پیشرفت‌های کلی در زمینه ی حمایت جزایی از مالکیت معنوی نیز حاصل شده است.

مرحله ی چهارم اصلاحات بین‌المللی قوانین، در مورد قوانین آئین‌دادرسی است. بسیاری از کشورها مانند آمریکا، کانادا، آلمان و دیگر کشورهای اروپایی قوانینی را در خصوص تفتیش و توقیف داده‌های رایانه‌ای وضع کرده‌اند. در این خصوص می‌توان به تدوین قوانین انگلیس در سال ۱۹۸۴، دانمارک ۱۹۸۵، آمریکا ۱۹۸۶ و هلند ۱۹۹۴ اشاره نمود.

مرحله ی پنجم اصلاح قوانین، در مورد جرائم مربوط به محتواست. به عنوان مثال بسیاری از کشورها قوانینی وضع کردند که تهیه، توزیع، عرضه و نگهداری پورنوگرافی(هرزه نگاری) کودکان از طریق سیستم‌ها و شبکه‌های رایانه‌ای را جرم تلقی کرده است.

در سال ۲۰۰۰ موسسه ی بین‌المللی مک کانل مطالعه‌ای در مورد وضعیت قوانین وضع شده در ارتباط با جرائم سایبری در چهار گوشه ی جهان به عمل آورده است .این موسسه از کشورها خواسته است که چنانچه قوانین و یا پیش‌نویس قوانینی در این خصوص دارند ارسال کنند، در غیر این صورت اعلام نمایند که هیچ اقدام مثبتی انجام نداده‌اند.

کشورهایی که قوانین خود را ارائه کرده‌اند به گونه‌ای مورد ارزیابی قرار گرفته‌اند که مشخص شود آیا قوانین جزایی آنها فضای شبکه‌های رایانه‌ای را شامل می‌شود یا نه؟ و آیا انواع جرائم سایبری را پوشش می‌دهد یا نه؟

سی و سه کشور (از بین بیش از ۵۰ کشور) مورد بررسی تا آن تاریخ نسبت به روز آمد کردن قوانین خود به منظور برخورد با انواع جرائم رایانه‌ای هیچ اقدامی انجام نداده بودند ولی اکثراً در حال تهیه ی پیش‌نویس قوانین بودند .این کشورها عبارتند از:

ایران، آلبانی، بلغارستان، بورندی، کوبا، دومینیکن، مصر، اتیوپی، فیجی، گامبیا، مجارستان، اردن، نیکاراگوئه، قزاقستان، لیتوانی، لبنان، لسوتر، مالت، مولداوی، مراکش، زلاندنو، نیجریه، رومانی، آفریقای جنوبی، ویتنام، یوگسلاوی، زامبیا، زیمبابوه.

ده کشور از کشورهای مورد بررسی برای برخورد با حداکثر پنج نوع از جرائم سایبری، قانون وضع کرده‌اند که عبارتند از: برزیل، کانادا، شیلی، چین، چک، دانمارک، مالزی، لهستان، اسپانیا و فرانسه.

نه کشور نیز برای برخورد با بیش از شش نوع از انواع جرم سایبری، قانون وضع کرده‌اند که عبارتند از: آمریکا، انگلیس، ترکیه، پرو، ژاپن، موریس، استونی، استرالیا و هند .

کشور فیلیپین برای اکثر جرائم سایبری قانون وضع کرده است.

از نیمه ی دوم دهه ی ۱۳۷۰ شمسی و بالاخص از ابتدای دهه ی ۱۳۸۰ که استفاده از رایانه های شخصی توسط سازمانهای اداری، موسسات خصوصی و افراد حقیقی در ایران گسترش یافته و دسترسی به خدمات متعدد اینترنت امکانپذیر شده، ارتکاب جرائم سایبری در کشورمان نیز از رشد نسبتا سریعی برخوردار بوده است. اشاعه ی فحشا و منکرات، انتشار عکس ها، تصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف بین اقشار جامعه از طریق طرح مسائل قومی و نژادی، انتشار مطالب نژاد پرستانه، انتشار اسناد و مسائل محرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افترا نسبت به مقامات دولتی، اشخاص حقیقی وحقوقی، سرقت ادبی وغیره از جمله جرائمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب سایتها و وبلاگها، پست الکترونیک، گروه های خبری، چت (گپ زدن) و سایر سرویسهای اینترنت بوقوع پیوسته اند. قانونگذار در سال ۱۳۷۹ در برابر برخی از جرائم سایبری واکنش نشان داده و با الحاق تبصره ی ۳ به ماده ی ۱ قانون مطبوعات مقرر داشته :کلیه ی نشریات الکترونیکی مشمول مواد این قانون است.

اولین واکنش قانونی ایران در برابر بعضی از جرائم سایبری، قانون اصلاح قانون مطبوعات مصوب ۱۳۷۹/۱/۳۰ مجلس شورای اسلامی می باشد که در تاریخ ۱۳۷۹/۲/۷مورد تائید شورای نگهبان قرار گرفته است.

دومین واکنش قانونی کشور ما در مقابل این نوع جرائم، از طریق وضع «قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ای» به عمل آمد. این قانون در تاریخ ۱۳۷۹/۱۰/۴ به تصویب مجلس شورای اسلامی رسید. ماده ی ۱۳ قانون مذکور نقض حقوق پدید آورندگان آن دسته از نرم افزارهای رایانه‌ای را که مورد حمایت این قانون قرار گرفته اند، جرم تلقی و برای آن مجازاتی معادل ۹۱ روز تا شش ماه حبس و جزای نقدی تعیین کرده است.

سومین عکس العمل قانونگذار ایران در مقابل جرائم سایبری در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ مجلس شورای اسلامی به عمل آمد. به موجب ماده ی ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تسلیم و افشاء غیر مجاز اطلاعات و داده‌ها به افرادی که صلاحیت دسترسی به آنرا ندارند، سرقت و یا تخریب حاملهای داده و سوء استفاده ی مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان، جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می‌شود.

چهارمین واکنش قانونی مرتبط با جرائم سایبری از طریق تصویب قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به موجب مواد۷۷، ۷۶، ۷۵، ۷۴، ۶۶،۶۷،۶۸،۶۹ این قانون، کلاهبرداری، جعل، دستیابی و افشاء غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی رایت) وغیره... که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی و برای آن مجازات تعیین گردیده است.

هر یک از چهار قانون فوق الذکر در بستر خاص خود قابلیت اعمال دارند .مثلا قانون مطبوعات صرفاً نسبت به جرائم سایبری ارتکابی در قالب نشریات الکترونیکی، قانون مجازات نیرو های مسلح صرفا در مورد بعضی از جرائم سایبری نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرائم سایبری ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند.

برای مقابله با سایر سوء استفاده‌های سایبری مانند سوء استفاده از محیط سایبر به منظور نفوذ به حریم خصوصی افراد، تخریب، سرقت، توقف و تغییر داده‌هایی که فاقد شرایط مقرر در قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای هستند، سوءاستفاده‌های مالی رایانه‌ای خارج از بستر تجارت الکترونیک و سایر سوء استفاده های رایانه‌ای، نیاز به یک قانون جرائم رایانه‌ای پیشرفته و جامع الاطراف است.

شورای عالی توسعه ی قضایی قوه ی قضائیه، پیش نویس قانون جرائم رایانه‌ای و آئین دادرسی آنرا در سال ۱۳۸۲ تهیه و طی جلسات متعددی با حضور حقوقدانان و متخصصان امور رایانه مورد بررسی قرار داد، تا پس از تصویب رئیس قوه قضائیه به عنوان لایحه ی جرائم رایانه‌ای از طریق هیئت دولت به مجلس شورای اسلامی تقدیم گردد. با این حال، سرعت تصویب و لازم‌الاجرا شدن قوانین حمایتی رایانه‌ای به هیچ وجه با توسعه ی کمی و کیفی این فناوری در کشورمان تناسب نداشته است و گام‌های نخستین قانونگذاری نیز شامل حوزه‌های محدودی نظیر حمایت از مالکیت فکری رایانه‌ای می‌شده که البته آنها نیز تمامی جنبه‌های حمایتی را در بر نمی‌گیرند. در همین راستا و با هدف تدوین یک قانون کیفری نسبتا جامع برای مقابله با سوء استفاده‌های سایبری، شورای عالی توسعه ی قضایی قوه ی قضاییه در ابتدای سال ۱۳۸۱ با همکاری شورای عالی اطلاع‌رسانی وقت، طرح تدوین لایحه ی مبارزه با جرائم رایانه‌ای را آغاز کرد. پس از آن، پیش‌نویس مذکور تقدیم رئیس وقت قوه ی قضاییه شد که در شورای عالی مسئولان قضایی مورد بررسی قرار گرفت و پس از تائید آن از سوی ایشان، تقدیم دولت شد که دولت نیز آنرا به مجلس شورای اسلامی تقدیم کرد. در سال ۱۳۸۴، کمیته ی تخصصی تشکیل شده در کمیسیون حقوقی و قضایی مجلس شورای اسلامی، متشکل از تعدادی از نمایندگان کمیسیون، لایحه را بررسی و تصویب کردند، لیکن نوبت به طرح لایحه در کمیسیون نرسید و عملا بررسی آن به دوره ی هشتم مجلس شورای اسلامی موکول شد. در شهریورماه ۱۳۸۷ کمیسیون حقوقی و قضایی مجلس به طور جدی لایحه را بررسی و تصویب کرد و جهت تصویب نهایی به صحن علنی مجلس ارجاع داد که تا پایان آن سال ادامه یافت و پس از یک بار ارجاع به شورای نگهبان و رفع ایرادهای مبتنی بر شرع و قانون اساسی وارده از

سوی آن شورا، نهایتا در تیرماه سال ۱۳۸۸ جهت دولت از سوی مجلس شورای اسلامی ابلاغ شد. این قانون مصوب، مشتمل بر ۳ بخش اصلی می باشد که به ترتیب به جرائم و مجازات‌ها، آئین دادرسی و سایر مقررات، اختصاص یافته‌است .

۳-۲ فعالیت سازمانهای بین‌المللی در خصوص جرائم سایبری

معمولاً سه محور برای حاکمیت بر اینترنت پیش‌بینی می‌شود محور اول کنترل و آزادی است، آزادی‌خواهان، معتقدان به حقوق بشر از جمله حامیان اصلی این محور به شمار می‌آیند. این عده هر چند معتقد به امکان کنترل اینترنت هستند لیکن به هیچ وجه قبول نمی‌کنند که این مسأله از حد کنترل به مراحل وخیم‌تر بعدی برسد. محور دوم عدالت در دسترسی است. دولت‌های گروه جنوب و شرکت‌های بزرگ بین‌المللی حامیان این محور هستند این دسته با اشاره به خطرات بالقوه‌ی کنونی در راه دسترسی به ثروت و قدرت همواره کوشیده‌اند تا حاکمیت بر اینترنت را از حد کنترل نیز فراتر روند لیکن محور سومی نیز وجود دارد که همواره به آن بی‌توجهی شده است این محور کاربران هستند آیا واقعاً کسی دیدگاه آنها را نیز مدنظر قرار خواهد داد؟تروریسم مجازی یکی از مشکلاتی است که همواره در مقابل اینترنت رخ نمایانده است. این مسأله از هک آغاز شده و به حمایت‌های دولتی از هکرها انجامیده است از جمله سازمان‌های بین‌المللی که در این باره دست به فعالیت‌هایی زده است اینترپول می‌باشد. این سازمان به همین علت سعی در تربیت پرسنل مجرب دارد تا با آشنایی به ظرایف کار بتوانند نقش‌آفرینی مناسبی در این خصوص داشته باشند سعی اینترپول بر این است تا با هر روش ممکن به کشورهای عضو کمک کند.ولی مؤسسه خدمات مصرف‌کنندگان محلی است که تا حدودی به فکر کاربران است این مؤسسه یک منشور ده ماده‌ای تهیه کرده است که هر چند زمینه‌های تجاری در آن غالب هستند لیکن می‌تواند راهنمای خوبی به شمار رود. از جمله این مواد حق شکایت و مطالبه خسارت در عملیات تجارت الکترونیکی است. همچنین صحت عمل و شرافت و تضمین آنها نیز در این منشور مورد تأکید قرار گرفته است.

به لحاظ خصیصه ی فراملی جرائم سایبری، اقدامات بین‌المللی فراوانی برای دستیابی به سیاست جنایی بین‌المللی ناظر بر این جرائم انجام شده است .فعالیت‌های بین‌المللی برای مبارزه با جرائم سایبری از دهه ی ۱۹۸۰ شروع شد .سازمان‌هایی مانند سازمان همکاری و توسعه ی اقتصادی، انجمن بین‌المللی حقوق جزا، سازمان ملل متحد، اینترپل، شورای اروپا و مجمع کشورهای شرکت‌کننده درکنفرانس بین‌المللی مبارزه با جرائم سایبر (۲۰۰۱) بوداپست، اقدامات ارزنده‌ای را در این خصوص انجام داده‌اند.

۱- سازمان همکاری و توسعه ی اقتصادی[11]

اولین کوشش بین‌المللی در مورد بحث و بررسی مشکلات حقوق جزا در برابر جرم سایبری توسط سازمان همکاری و توسعه ی اقتصادی صورت پذیرفت. این سازمان در سال ۱۹۷۷ شروع به اتخاذ رهنمودهایی ناظر به حمایت از حقوق فردی و جریان فراملی داده‌های شخصی کرد. کمیته ی تخصصی این سازمان، کار خود را در زمینه ی ایجاد هماهنگی بین‌المللی بین قوانین

---

[11] - Organization for Economic Cooperation and Development

سازمان همکاری و توسعهٔ اقتصادی(OECD)سازمانی است بین‌المللی، دارای ۳۵ عضو، که اعضای آن متعهد به اصول دموکراسی و اقتصاد آزاد هستند. این سازمان به تعبیری عمده‌ترین سازمان بین‌المللی تصمیم‌گیرندهٔ اقتصادی است. مقرّ اصلی این سازمان در شهر پاریس است .
این سازمان در سال ۱۹۴۸ میلادی تحت عنوان *سازمان همکاری اقتصادی اروپا* تأسیس شد. این مؤسسه تحت مدیریت رابرت مارژولین فرانسوی به‌منظور اجرای طرح بازسازی کشورهای اروپایی بعد از جنگ جهانی دوم ایجاد شد؛ طرحی که تحت عنوان *برنامهٔ مارشال* توسط ایالات متحدهٔ آمریکا برای بازسازی اروپا بعد از جنگ و مبارزه با کمونیسم برنامه‌ریزی شده بود. در سال‌های بعد، اعضای غیر اروپایی نیز به این سازمان پیوستند و در سال ۱۹۶۱ میلادی در اجلاسی با تصویب آیین‌نامهٔ جدید در زمینهٔ توسعه و اقتصاد، نام سازمان را نیز به سازمان همکاری و توسعهٔ اقتصادی تغییر دادند .

کیفری برای مبارزه با جرائم اقتصادی رایانه‌ای شروع کرد و در سال ۱۹۸۹ لیستی از سوء استفاده‌های رایانه‌ای را ارائه داد. در سال ۱۹۸۹ این سازمان کارش را در خصوص امنیت سیستم‌های رایانه‌ای ادامه داد.

۲- سازمان ملل متحد[۱۲]

در هفتمین کنگره ی سازمان ملل متحد در سال ۱۹۸۵ "جرم سایبری" از جمله موارد مطروحه در گزارش دبیر کل این سازمان بود. به عنوان برنامه ی تدارکاتی هشتمین کنگره ی سازمان ملل متحد، اجلاس مقدماتی منطقه‌ای آسیا و اقیانوس آرام، نگرانی خود را درباره ی آثار پیشرفت‌های تکنولوژی و انعکاس آن در جرائم سایبر اعلام داشت. در اجلاس مقدماتی منطقه‌ای اروپا پیشنهاد شد که مبارزه ی بین‌المللی با جرائم رایانه‌ای از سوی هشتمین کنگره ی سازمان ملل متحد و کنگره‌های پس از آن مورد حمایت و توجه قرار گیرد. در دوازدهمین اجلاس عمومی کنگره ی هشتم که در سال ۱۹۹۰ برگزار شد، نماینده ی کانادا پیش‌نویس قطعنامه‌ای را در مورد جرائم رایانه‌ای تسلیم کنگره کرد. در سیزدهمین اجلاس عمومی کنگره ی هشتم، قطعنامه ی مذکور پذیرفته شد. در این قطعنامه از کشورهای عضو خواسته شده است که به تلاشهای خود در زمینه ی مبارزه با جرائم رایانه‌ای از طریق مدرنیزه کردن قوانین و دادرسی های ملی، ارتقاء ضوابط پیشگیرانه و امنیتی رایانه، اتخاذ تدابیری برای ایجاد حساسیت در مردم و قوه ی قضائیه برای جلوگیری از جرائم رایانه‌ای و... شدت بخشند و از دبیر کل سازمان خواسته شد تا موضوع انتشار یک نشریه ی فنی در مورد جلوگیری و تعقیب جرائم رایانه‌ای را مد نظر قرار دهد.

مجمع عمومی سازمان ملل متحد در قطعنامه ی شماره ۴۵/۱۲۱ خود اسناد و قطعنامه‌های مصوبه ی هشتمین کنگره را پذیرفت و از دولتها خواست تا در تبیین قوانین و دستورالعمل‌های تعیین‌کننده ی خط مشی خود و براساس شرایط اقتصادی، اجتماعی، حقوقی، فرهنگی و سیاسی در کشور از قطعنامه‌های مزبور تبعیت کنند.

۳- انجمن بین‌المللی حقوق جزا [۱۳]

انجمن بین‌المللی حقوق جزا که یک سازمان غیر دولتی است در سال ۱۹۹۰ جرم سایبری را به عنوان یک موضوع مورد بحث برای اعضای خود مطرح کرد. در سال ۱۹۹۲ یک نشست مقدماتی پیرامون این جرم در دانشگاه ورتسبورگ آلمان برگزار و قطعنامه‌ای در مورد فهرست جرائم رایانه‌ای صادر کرد. در سال ۱۹۹۴ در نشست نهایی خود در ریودوژانیرو و در نشستهای بعدی خود مصوباتی در این خصوص داشته است.

۴- یونسکو[۱۴]

در اجلاس سال ۱۹۹۹ یونسکو در پاریس که با حضور ۳۰۰ نفر از متخصصان در حوزه ی مراقبت و محافظت از اطفال، متخصصان اینترنت و تهیه‌کنندگان خدمات اینترنتی و..... به منظور بررسی راههای مبارزه با سوء استفاده ی جنسی از اطفال،

---

12 - United Nations

13 - International Criminal Law Society**:**

انجمن بین‌المللی حقوق جزا(**ICLS**) از جمله سازمانهای بین‌المللی غیر دولتی **(NGO)** محسوب می‌شود که حدود یکصد و پانزده سال عمر دارد و در حوزه حقوق بین الملل کیفری فعالیت می نماسد.. در حال حاضر انجمن بیش از سه هزار عضو دارد و علاوه بر آن چهل گروه ملی حقوق جزا از کشورهای مختلف جهان نیز عضویت آن را دارا می‌باشند.

14 -UNESCO**:**

سازمان آموزشی، علمی و فرهنگی ملل متحد ،(The United Nations Educational, Scientific and Cultural Organization)که به‌طور خلاصه یونسکو **(UNESCO)**نامیده می‌شود، یکی از سازمان‌های تخصصی وابسته به سازمان ملل متحد است که در سال ۱۹۴۵ تشکیل شد. هدف این سازمان کمک به صلح و امنیت در جهان از راه همکاری بین‌المللی در زمینه‌های آموزشی و علمی و فرهنگی و تربیتی به منظور افزایش احترام به عدالت و قانون‌مداری و حقوق بشر، بر پایه منشور سازمان ملل متحد است.

پدوفیلی[15] (کودک دوستی به منظور سوء استفاده ی جنسی) و هرزه نگاری اطفال در اینترنت تشکیل شد، اعلامیه ی مورخه ۱۹۹۹/۱/۱۹ یونسکو که یک برنامه ی عملی برای مبارزه با جرائم اینترنتی علیه اطفال می باشد، صادر گردید.

۵- شورای اروپا

شورای اروپا در سال ۱۹۸۵ موضوع جرم رایانه ای را از طریق یک کمیته ی تخصصی مورد مطالعه و بررسی قرار داده است. کمیته ی منتخب کارشناسان جرم رایانه‌ای کار خود را در سال ۱۹۸۵ شروع و در سال ۱۹۸۹ یک توصیه نامه و یک گزارش به کمیته ی اروپایی مسائل ناشی از جرم ارائه کرد. کمیته نیز پس از تصویب، آنرا به کمیته ی وزرای شورای اروپا فرستاد و در سپتامبر ۱۹۸۹ به عنوان یک توصیه نامه تحت عنوان(R ۹۸۹)مورد تصویب نهایی قرار گرفت. توصیه نامه ی دیگری در زمینه ی آئین‌دادرسی جرائم فناوری اطلاعات در سال ۱۹۹۵ تحت عنوان توصیه نامه ی(R ۱۳۹۵)توسط این شورا تصویب شده است.

کمیته ی وزراء شورای اروپا درسال ۱۹۹۷ کمیته ی دیگری به نام کمیته ی متخصصان جرائم سایبر را تشکیل داد. این کمیته پیش‌نویس کنوانسیون جرائم سایبر و گزارش توجیهی آنرا در سال ۲۰۰۰ تهیه کرد.

کنوانسیون جرائم سایبر درسال ۲۰۰۱، در یک کنفرانس بین‌المللی که با شرکت کشورهای عضو شورای اروپا و چهار کشور دیگر (آمریکا، ژاپن، آفریقای جنوبی و کانادا) تشکیل گردید، به تصویب رسید که کاملترین سند بین‌المللی در مورد جرائم رایانه‌ای است.

۶- ITV دیگر سازمان بین‌المللی است که سعی در ایجاد قواعد بین‌المللی داشته و دارد. در سال ۱۹۸۲ نخستین کنفرانس جهانی توسعه ارتباطات دور توسط اتحادیه مذکور و در سطح وزرا تشکیل شد. این اجلاس در نایروبی برگزار شد و پس از آن بود که مرکز توسعه ارتباطات دور رسماً افتتاح شد. از جمله اقدامات این مرکز گزارشی با عنوان (دگرگونی محیط ارتباطات دور) بود که توسط گروه مشورتی سیاست‌های ارتباطی ITV منتشر شد این گزارش در سال ۱۹۸۹ منتشر شد.سال ۱۹۹۹ در ایالات متحده قانون حمایت مصرف‌کننده در مقابله با غصب الکترونیکی به تصویب رسید. هر چند این مصوبه یک قانون ملی بود لیکن WIPO[16]از این قواعد و همچنین قواعد تنظیم شده توسط ICANN استفاده می‌کرد و بدین وسیله آنها را به سطح بین‌المللی می‌آورد. این مسأله به خاطر توافقنامه‌ای بود که این سازمان بین‌المللی با[17] ICANN منعقد کرده بود و طی آن اختلافات ناشی از ثبت نام‌های با سطح ژنریک بالا به WIPO منتقل می‌شد. مرکز داوری وایپو سالانه قریب به ۱۰ها هزار اختلاف این چنینی را حل و فصل می‌نمود در قانون مذکور که توسط ایالات متحده تصویب و توسط وایپونیز اجرا می‌گردید حقوق بهره‌برداران از اینترنت اعلام شده بود از جمله این حقوق عبارت بودند از: حق برخورداری از ایمنی، حق برخورداری از اطلاعات کامل، حق برخورداری از حمایت دولت‌ها، حق انتخاب و حق جبران خسارت.

۳-۳ راهکارهای پیشگیرانه جرایم سایبری در حقوق بین الملل

---

[15] - *پدوفیلی* (**Pedophilia**). پدوفیلیا یعنی اختلال روانی که مشخصه آن فانتزی یا عمل واقعی درگیر شدن در فعالیت جنسی با کودکان است. افراد *پدوفیل* فعالیت جنسی با کودکان را یا ترجیح می‌دهند و یا به طور منحصر به فرد از فعالیت جنسی با کودکان از همان جنس یا کودکان از جنس دیگر به هیجان جنسی و لذت بردن دستیابی پیدا می‌کنند.

16 - World Intellectual Property Organization:سازمان جهانی مالکیت معنوی

17 - Internet Assigned Numbers Authority

آیکان**(ICANN)** ، شرکت اینترنتی برای نامها و شماره‌های واگذار شده شرکتی غیرانتقاعی است که مقر آن در منطقه مارینا دِل رِی شهر لس آنجلس ایالت کالیفرنیا در ایالات متحده آمریکا واقع شده، در تاریخ ۱۸ سپتامبر ۱۹۹۸ ساخته شده و در ۳۰ سپتامبر ۱۹۹۸ برای اینکه قادر به سرپرستی بخشی از وظایف مربوط به اینترنت که پیشتر مسوولیت انجام آن مستقیما به عهده دولت ایالات متحده بوده و بوسیله سازمان‌های دیگر انجام می‌شده باشد ثبت شد

افزایش روزافزون جرایم در فضای سایبر و آسیب ها و پیامدهای مخرب اجتماعی ، فرهنگی ، اخلاقی، سیاسی و اقتصادی آن ،دولتها و سازمانهای بین المللی را به تکاپو واداشته تا با اتخاذ سیاستها ی کنترلی ورویه های حقوقی به مبارزه با جرایم سایبری بپردازند .آنچه در ادامه از نظرتان می گذرد مروری بر الگوها ومدلهای ملی و بین المللی مقابله با جرایم سایبر است .

الف)کنترل دولتی

در این روش، سیاست کلی حاکم بر کشور اجازه ی دسترسی به پایگاههای مخرب و ضد اخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازه ی اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند.

ب) کنترل سازمانی

روش دیگر، کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرند، خود موظف به کنترل شبکه و نظارت بر استفاده ی صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی تواماً انجام این وظیفه را تضمین کند.

ج)کنترل فردی

کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل تمام تضمینهای اجرایی، درون فردی است و شخص با بهره‌گیری از وجدان فردی، مبانی اخلاقی و تعهد دینی، مراقبتهای لازم را در ارتباط با شبکه‌های جهانی به عمل آورد. این اعتقاد و فرهنگ در محدوده ی خانواده نیز اعمال می‌شود. البته شیوه ی اخیر در صورتی ممکن خواهد بود که واگذاری خط اشتراک[۱۸] IP پس از شناسایی کامل افراد و با ملاحظه ی خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند.

د)وجود یک نظام قانونمند اینترنتی

مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیبهای اینترنتی از قبیل اطلاعات نادرست و یا پیامدهای ضد اخلاقی نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که اداره ی آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسار گسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری نماید. این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تاثیرپذیری از فرهنگهای بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد.

ه)سیاست‌گذاری ملی در بستر جهانی

واقعیت این است که بدون ملاحظه ی چند الگوی ملی در برخورد با اینترنت نمی‌توان از سیاست‌گذاری مبتنی بر فهم جهانی سخن گفت. لذا معرفی اجمالی چند نمونه که با سه رویکرد تحول‌گرا، ثبات‌گرا و اعتدال‌گرا تناسب بیشتری دارند ضروری است.

۱- الگوی آمریکایی

اینترنت در آمریکا هم به عنوان تهدید امنیتی و هم به عنوان بزرگترین فرصت ملی تلقی می‌شود. کاخ سفید در پنجم ژانویه سال ۲۰۰۰ بیانیه‌ای را تحت عنوان «استراتژی امنیت ملی در قرن جدید» منتشر کرد. در این بیانیه ضمن برشمردن منافع حیاتی آمریکا، از اینترنت به عنوان مهمترین ابزار دیپلماسی مردمی نام برده شده است. پیشرفت جهانی تکنولوژیهای آزاد و اطلاع‌رسانی چون اینترنت توانایی شهروندان و موسسات را برای تاثیرگذاری بر سیستمهای دولتها تا حد غیرقابل تصوری بالا

---

[۱۸] - نشانی پروتکل اینترنت یا به اختصار نشانی آی‌پی **(IP Address)** نشانی عددی است که به هریک از دستگاه ها و رایانه‌های متصل به شبکه ی رایانه ای که بر مبنای نمایه **TCP/IP**از (جمله اینترنت) کار می‌کند، اختصاص داده می‌شوند. پیام‌هایی که دیگر رایانه‌ها برای این رایانه می‌فرستند با این نشانه ی عددی همراه است و راه یاب های شبکه آن را مانند «نشانی گیرنده» در نامه‌های پستی تعبیر می‌کنند، تا بالاخره پیام به رابط شبکه رایانه مورد نظر برسد.

برده است. دیپلماسی مردمی یعنی تلاش برای انتقال اطلاعات و پیامهایمان به مردم جهان. توسعه ی اینترنت در داخل و استفاده از آن برای تاثیرگذاری بر دیگران بخش مهمی از سیاستهای استراتژیک آمریکاست.

۲-الگوی فلسطین اشغالی

این کشور در فاصله ی سال ۱۹۹۴ تا ۲۰۰۰ تبدیل به یک غول صنعت اینترنت شده است. فلسطین اشغالی در سطح داخلی سیاستهایی اتخاذ کرده که عبارتنداز:

-اختصاص ۳٪ از[۱۹] GDP کشور معادل ۹۰ میلیارد دلار به تحقیق و توسعه در زمینه ی تکنولوژی پیشرفته.

-آموزش مهارتهای پیشرفته ی رایانه‌ای در دوران سربازی و تداوم آموزش در دوران خدمت احتیاط.

-تولید Checkpoint با پیشینه و ریشه در کاربردهای نظامی و به عنوان یکی از قابل اطمینان‌ترین و پرفروشترین باروهای جهان (فایروال یا بارو، شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها)هکرها) و وب سایتهای نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و دارایی های افراد را از دسترس نیروهای متخاصم دور نگاه می‌دارد (که کشورهای عربی نیز به آن متکی هستند، یکی از سیاستهای جهانی کشور مذکور است.

۳-الگوی چینی

چین رسماً اعلام کرده به دنبال برقراری توازن میان جریان آزاد اطلاعات و صیانت فرهنگ و ارزشهای اجتماعی خود می‌باشد. در اجرای این استراتژی، چین اقدامات زیر را انجام داده است:

-سرمایه‌گذاری عظیم در صنایع الکترونیک، مخابرات و رایانه

-اقدامات وسیع و سازمان یافته برای تکثیر، شکستن قفل و شبیه‌سازی نرم‌افزارها و برنامه‌های کاربردی رایانه‌ای و تقویت صنعت عظیم نرم‌افزار در چین.

-تاسیس شرکت دولتی اینترنت چین و انحصار ورود اینترنت به کشور از طریق این شرکت

-همکاری شرکت با غولهای اینترنتی آمریکا برای ایجاد خدمات مبتنی بر وب با استانداردهای کیفی AOL[۲۰] و استانداردهای اخلاقی و قانونی چین

-جلب همکاری AOL و Netscape[۲۱] برای تولید یک پویشگر اینترنت به زبان چینی

-هزینه ی عظیم برای فیلتر کردن محتوای نامناسب اخلاقی و سیاسی در اینترنت

۴-اصول حقوق بین الملل در مقابله با جرایم سایبری

۴-۱ اصول صلاحیت کیفری مربوط به مجرمان بین المللی

همانطور که قبلا ذکر شد، جرایم سایبری فراتر از مرزهای جغرافیایی اتفاق می افتند و در نتیجه، محل اصلی ارتکاب جرم و کشور آسیب دیده ممکن است متفاوت باشند. برای مثال اگر شخص Aبا ملیت فیلیپینی، ویروسی در فیلیپین منتشر کند و

---

[19] - gross domestic product:تولید ناخالص داخلی

[20] - acceptable auality level

سطح کیفی قابل قبول :درصدی از نقایص در یک تناوب زمانی از پیش معین که در روند نمونه برداری و در هنگام بازرسی یا آزمایش محصول یا سیستم پذیرفته میشود

[۲۱] - نت‌اسکیپ: شرکت خدمات کامپیوتری آمریکایی است، که در زمینه ارائه مجموعه نرم‌افزارهای اینترنتی، مرورگر وب، پورتال‌های وب و خدمات اینترنتی فعالیت می‌نماید.

این ویروس به شرکت Bدر ایالات متحده آسیب بزند، این مسئله پیش می آید که این فرد باید بر طبق قانون کدام کشور مجازات شود.

اصول صلاحیت کیفری اعمال مجرمانه بین المللی به چند دسته اقلیمی، صلاحیت شخصی فعال، صلاحیت شخصی منفعل، حمایت گرایی و جهانی گرایی تقسیم شده اند .بر اساس مثال بالا به شرح هر کدام از این اصول می پردازیم.

الف)اصل صلاحیت سرزمینی

این اصل به معنی اعمال قانون ملی به تمام جرایم مرتکب شده در قلمرو یک کشور، صرف نظر از ملیت مجرمان،گفته می شود. با توجه به این اصل، وقتی فرد A در فیلیپین مرتکب جرمی می شود، برای مجازات این شخص باید قانون کشور فیلیپین اعمال شود. با این حال، بر اساس اصل حضور همه جانبه، اگر این جرم در امریکا هم اتفاق افتاده باشد، چه بسا اجرای قانون در اختیار و صلاحیت این کشور باشد. اگر فیلیپین هیچ قانونی برای مجازات این جرم نداشته باشد، پس در نتیجه این عمل در فیلیپین جرم محسوب نمی شود. در نتیجه می توان گفت حوزه قضایی این جرم به فیلیپین محدود نمی شود.

ب) اصل صلاحیت شخصی

اصل صلاحیت شخصی فعال صرف نظر از محل ارتکاب جرم، به اعمال قانون کشور فرد مجرم اطلاق می شود. بر اساس این اصل اگر چه جرم شخص A در امریکا صورت گرفته باشد، و خود فرد دارای ملیت فیلیپینی باشد، فقط فیلیپین صلاحیت رسیدگی به این جرم را دارد، نه امریکا. در صورتی که فیلیپین هیچ قانونی برای رسیدگی به این جرم نداشته باشد، این عمل جرم محسوب نشده و به اصل مشروعیت ارجاع داده می شود.

ج)اصل صلاحیت شخصی منفعل

این اصل می گوید که دادگاه کشور قربانی صلاحیت رسیدگی به این جرم را دارد. با توجه به این اصل، کشور قربانی B یا همان امریکاست که دارای صلاحیت داوری است نه فیلیپین. با این حال، این اصل در سطح بین المللی مورد استفاده قرار نگرفته و هیچ معاهده ای بر اساس آن وجود ندارد.

د)حمایت گرایی

سیستم حمایتی به این معنی است که صرف نظر از کشوری که مرتکب جرم شده و کشور قربانی، قانون کشور مورد نظر به هر کدام از اعمال مجرمانه که حقوق آن کشور را نقض کرده است اعمال شود. بر اساس این اصل، شرکت B در امریکا است که اقدام مجرمانه A باعث به خطر افتادن حقوق آن شده است که به حوزه قضایی فدرال مربوط می شود. با این حال، جرائم مربوط به Rechtsgut ملی تحت قانون هر دو کشور قرار می گیرند. که حوزه قضایی فدرال در پشتیبانی و حمایت از آنها مختار است.

ه) جهانی گرایی

جهانی گرایی استفاده از کشور برای یک عمل خاص مجرمانه (دزدی دریایی، جنگ، و غیره) صرف نظر از کشور محل وقوع جرم و جنایت و مجرم و قربانی است .در این حالت، اعمال مجرمانه معین در چارچوب جهانی گرایی شامل دزدی دریایی، جنگ و جرم علیه بشریت است که توسط عوامل بین المللی تشخیص داده می شود .بنابراین، بر اساس این قانون، امریکا سازوکار رسیدگی به جرایم اینترنتی را ندارد.

۲-۴ مشکلات انعقاد کنوانسیون صلاحیت کیفری برای جرایم سایبری بین المللی

همانطور که قبلا ذکر شد، اگر یک جرم اینترنتی بین المللی رخ دهد مسائل بسیاری ممکن است در مورد صلاحیت کیفری این جرم بوجود بیاید. موثر ترین راه برای حل این مشکل ایجاد یک اصل واحد برای احراز صلاحیت در حوزه جرایم سایبری جهانی بر اساس قوانین بین المللی است. با این حال، هنوز هم، اجرای چنین اصلی مشکل به نظر می رسد.

همانطور که در بالا گفته شد، جرایم اینترنتی بین المللی بدون در نظر گرفتن مکان و زمان در فضای بین المللی سایبری اتفاق می افتند. تحت این شرایط، حتی اگر یک معاهده بین المللی دراحراز صلاحیت کیفری جرایم اینترنتی بین المللی نیز وجود داشته باشد، اگر تمام کشورهای جهان در آن مشارکت نداشته باشند، این معاهده بیهوده خواهد بود.

در صورت بروز عمل مجرمانه، به لحاظ اینکه رویه قضایی جنایی در معاهده ای قطعیت یابد تمام کشورهای مشارکت کننده می توانند بر اساس یک اصل واحد کنترل داخلی و خارجی موثر بر جرم داشته باشند. در مقابل؛ زمانی که جرایم اینترنتی بین المللی در فضای مجازی توسط مجرمان انجام شود و کشور مربوطه به این معاهده ملحق نشده باشد، آن کشور ضرورتا نیازی ندارد که با آن رویه قضایی رسیدگی به جرم که معاهده آن را تعریف کرده هماهنگ شود. در نتیجه جرایم اینترنتی بدون مرز هستند و برای استاندارد سازی رویه های قضایی حاکم بر این جرائم نیازمند قوانین و مقررات یکسان و جهانی هستیم. معاهده های المللی بر اساس مشارکت داوطلبانه ملی نمی تواند تضمین کننده مشارکت همه کشورها باشد بنابر این و در واقعیت کنترل جرایم اینترنتی از این طریق بسیار دشوار است.

۳-۴ مشکلات درباره صلاحیت کیفری بین المللی جرایم سایبری

الف) حل مشکل از طریق قوانین بین المللی جاری

دشوار است که یک داوری بین المللی بر اساس مشارکت ملی در واقعیت یک الزام عمومی داشته باشد بنابر این بهتر است حل مسائل مربوط به جرایم اینترنتی بین المللی از طریق قوانین بین المللی متعارف صورت بگیرد تا معاهدات. وقتی از وضع یک قانون بین‌المللی متعارف صحبت کی‌کنیم، این امر نیازمند یک همانندی جهانی نیست بلکه به محض اینکه این قانون به وجود می‌آید عوامل الزام آور کلی را شکامل می‌شود. بنابر این معقول است اصول یکسانی بر قوانین جرائم انترنتی بی‌المللی از طریق الزامات قوانین معمول بین‌المللی اعمال شود .

۱- الزامات قانون جاری در حقوق بین المللی رایج

قوانین جاری بین‌المللی به طور عمده بر اساس شیوه‌های ملی مستقر می‌شود اما همه آنها به یک قانون جاری تبدیل نمی‌شوند. در پروسه تبدیل شدن به یک قانون رایج، باید "شیوه های عمومی" شامل تداوم، همسانی، و کلیت در نظر گرفته شوند. همچنین، کشور مورد نظر باید دارای تاییدیه حقوقی در آن بخش باشد. دیوان بین المللی دادگستری (ICJ)[۲۲] برای الزاماتی را برای استقرار حقوق بین الملل جاری را اعلام کرده است.

در این حکم، دیوان بین المللی دادگستری به این نتیجه رسیده است که برای برخی از مفاد معاهده به عنوان یک حقوق بین الملل رایج باید شرایط زیر برقرار شود: ۱- آن ماده از قانون باید دارای ویژگی ایجاد هنجار باشد ۲ -مشارکت کشورها خصوصا کشورهایی که منافع آنها به طور ویژه ای به این عمل وابسته است ۳- عملکردهای کشور مورد نظر گسترده و سازگار باشد ۴- این شیوه ها به عنوان وظایف قانونی تلقی شوند.

آنچه که در اینجا نیاز به توجه دارد اهمیت" کشورهایی است که منافع آنها مستقیما تحت تاثیر قرارمی گیرد." برای اینکه اقدامات کلی به نوبه خود به حقوق بین الملل رایج تبدیل شوند، باید برای یک دوره معینی از زمان، حفظ و نگهداری شوند. با این حال، هیچ دوره زمانی ثابتی برای تشکیل آداب و رسوم و شیوه های آن وجود ندارد. به این ترتیب قوانین جاری و عمومی که در کشورها ایجاد شده اند، در دوره ای کوتاه امکان تبدیل شدن به قوانین رایج، "گسترده و در واقع سازگار" را دارا هستند.

---

[22] - **International Court of Justice**:

دیوان بین‌المللی دادگستری معروف به دادگاه جهانی رکن قضائی اصلی سازمان ملل متحد است که مقر آن در کاخ صلح شهر لاهه در کشور هلند واقع شده‌است. رسیدگی به اختلافات قانونی میان کشورها به این دادگاه ارجاع می‌شوند و همچنین ارائه نظر مشورتی در پاسخ به سوالات حقوقی سازمان‌های بین‌المللی، آژانس‌های تخصصی سازمان ملل و مجمع عمومی ملل متحد از وظایف اصلی این دیوان است.

1.3ارائه دستورالعمل از طریق سازمان ملل متحد و وضع قوانین بین المللی متعارف

برای ایجاد حقوق بین الملل رایج درباره صلاحیت رسیدگی کیفری به جرایم اینترنتی بین المللی، باید شیوه های ثابتی وجود داشته باشد. به طور کلی، منظور از شیوه، عملکرد یکنواخت و مداوم در کشورهاست. یکی از موثر ترین راه ها برای شکل‌گیری این شیوه این است که یک راهنمای جهانی در بازتاب نظرات کشورهایی که دارای منافع خاص در حوزه جرایم اینترنتی بین المللی هستند ایجاد و منتشر کرد، اما هنوز هیچ نظام قانوی الزام آور معتبری وجود ندارد ،به نظر می‌رسد چنین شیوه‌نامه ای توسط یک سازمان بی‌المللی جهانی که آن را سازمان ملل می‌نامیم تدوین شود. برای جزئیات این دستورالعمل، برای کشورهایی که تحت تاثر قرار می‌گیرند معقول است که رویه‌های قضایی منطبق با اصل قلمرو و اصل شخص غیر فعال داشته باشند. دستورالعمل فوق امکان توسعه یافتن به حقوق بین الملل رایج را به دلایل زیر دارا می باشد: ۱- اصل یکسان سازی قضایی برای جرائم انترنتی بین‌المللی سایبر این است که به طور اساسی دارای ویژگی هنجارآورینی است ۲- کشورهای آسیب دیده از جرم بین المللی سایبر به آن دسته از کشورهایی محسوب می‌شود که دارای منافع خاص هستند و مشارکت این قبیل کشورها توصیه می‌شود. و اگر قرار است این رویه ها شکل بگیرند باید :۱- به طور گسترده ای، به آن عمل شود ۲- تحت اطمینان حقوقی کشورهای مشارکت کننده انجام شوند. در نتیجه این دستور العمل به عنوان حقوق بین الملل جاری قابل ثبت خواهد بود.

نتیجه گیری

با توجه مطاب مرقوم شده، توسعه فناوری، اینترنت و ارتباطات و تجارت رایانه ای، ، عرصه نوینی از فعالیت های انسانی را بازکرده و موجب تضعیف مشروعیت قوانین بر اساس مرزهای جغرافیایی شده است. مقالات و کتب منتشره در سال های اخیر تاثیر شگرفی در توجه جهانیان به این جبهه جنگی داشته است. نوشتار حاضر به دنبال پاسخگویی به این سوال کلیدی است که جنگ سایبری چیست و آیا اقدامات مخرب سایبری از سوی کشورها می توانند موجد عناصر تجاوز و مشمول جرائم بین المللی، توسل به زور و بالتبع مسئولیت بین المللی دولت ها باشند؟ جهت یافتن پاسخ به چنین پرسشی باید به جستجو در اسناد بین المللی همچون منشور ملل متحد، کنوانسیون های حقوق جنگ و حقوق بشردوستانه و همچنین دستورالعمل تالین در خصوص جنگ های سایبری پرداخت. هرچند دستورالعمل اخیر، از نظر جرم انگاری و ارائه راهکار، با وجود کپی برداری از مواد کنوانسیون های با موضوع بشردوستانه، بالنسبه جامع و کامل بوده اما ماهیت ارشادی آن، مانع بزرگی در برابر لازم الاجرا و آمره بودن آن می نماید. با این وجود، بررسی آن به عنوان تنها منبع بین المللی با موضوع حقوق بین الملل قابل اعمال در نبردهای سایبری، خالی از لطف به نظر نمی رسد. ارتباطات رایانه ای جهانی (اینترنت) که در فضای مجازی صورت می گیرد، مرزهای جغرافیایی را در هم شکسته و قلمرو جدیدی برای فعالیتهای بشری بوجود آورده است. بگونه ایکه امکان بکارگیری حقوق موجود در چاچوب مرزهای ملی را تضعیف نموده است. با توجه به نفوذ اینترنت در عرصه های مختلف حقوقی، سیاسی، مالی، تجاری و اجتماعی جوامع بشری، دولتها خود را ناگزیر از قانونمند نمودن اینترنت دیده و به فراخور حال خود قوانین داخلی و بین المللی برای این فضا وضع نموده اند. لکن ماهیت فرامرزی و ابعاد بین المللی اینترنت باعث شده تنظیم آن توسط حاکمیتهای مختلف موجب اصطکاک صلاحیتها شده و ابهامات حقوقی این فضا افزوده شود. بنابراین تلاش یکجانبه دولتها برای قانونمند نمودن اینترنت بدون همکاری بین المللی بی حاصل خواهد بود.

با توجه به اقدامات تقنینی و پیشگیرانه توسط دولت ها در حوزه ملی و همچنین دولتها در قالب کنوانسیون ها در عرصه بین الملل،سعی شده تا این فضا نیز به مثابه فضای فیزیکی به نظم درامده و قانونمند گردد،ولی گاها به دلیل شتابزدگی های قانونگذاری و عدم شناخت کافی قانونگذار به ماهیت این فضا ،باعث ایجاد خلاء های قانونی در فضای مجازی گردیده است.

در این راستا توجه ویژه به تدابیر پیشگیرانه غیرکیفری و توسعه ی عدالت ترمیمی به جای عدالت کیفری و مجازات های بی فایده از اهمیت بالایی برخوردار است . در این راستا با نگاه ویژه به اصل پیشگیری غیرکیفری از جرم اعمّ از اجتماعی ووضعی پیشنهاداتی ارایه میگردد که امید است با اجرای این اقدامات و توسعه تحقیقات و بررسی های علمی در زمینه فضای مجازی شاهد کاهش یا ریشه کن شدن جرایم سایبری باشیم.

منابع

الف) فارسی

۱- افروغ، عبدالمحمد و زارعی،مصطفی، (۱۳۹۵)،بررسی اعمال صلاحیت کیفری در رسیدگی به جرایم سایبری در حقوق ایران و اسناد بین الملل، دومین همایش بین المللی پژهش های نوین در هزاره سوم، دانشگاه شیراز،۳۱ اردیبهشت۹۵

۲-بختیاری، نوبخت، (۱۳۹۰)، مقایسه چالش های دادرسی جرایم رایانه ای با جرایم سنتی، همایش منطقه ای چالش های جرایم رایانه ای در عصر امروز، انجمن علمی و ادبی و هنری دانشگاه آزاد اسلامی واحد مراغه.

۳- بیگی،جمال،(۱۳۹۰)، جرایم رایانه ای و مقابله با آن در اسناد بین الملل،همایش منطقه ای چالش های جرایم رایانه ای در عصر امروز،انجمن علمی و ادبی و هنری دانشگاه آزاد اسلامی واحد مراغه.

۴-پاکزاد، بتول(۱۳۸۸).«تروریسم سایبری ». رساله دکتری حقوق جزا و جرم- شناسی،دانشکده حقوق دانشگاه شهید بهشتی.

۵- تحریری،حمیدرضا،(۱۳۸۹)، جایگاه فضای مجازی در حقوق بین الملل، پایان نامه کارشناسی ارشد دانشگاه تهران

۶-جلالی فراهانی،امیرحسین و باقری اصل،رضا(۱۳۸۶).«پیشگیری اجتماعی از جرایم وانحرافات سایبری».مجله مجلس وپژوهش،شماره ۵۵،۱۲۴.

۷-جلالی فراهانی، امیرحسین، (۱۳۸۹)،کنوانسیون جرایم سایبر و پروتکل الحاقی آن (به همراه گزارش های توجیهی آنها) ، معاونت حقوقی و توسعه قضایی قوه قضائیه، تهران : نشرخرسندی، چاپ نخست،

۸-جینا،دی‌آنجلیز(۱۳۹۱).«جرایم سایبر».مترجمین: سعید حافظی، عبدالصمد خرم آبادی،چاپ نخست،تهران:انتشارات ققنوس.

۹- حسن بیگی، ابراهیم،(۱۳۸۲)، آسیب‌شناسی شبکه جهانی اطلاع‌رسانی اینترنت و ارائه راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تاکید بر جنبه‌های حقوقی و فنی، پایان‌نامه دکتری، دانشگاه عالی دفاع ملی.

۱۰- حسینی، بیژن،(۱۳۸۲)، جرائم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن، پایان‌نامه مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم تحقیقات.

۱۱-حسن حیدری،(۱۳۹۲). «اعمال صلاحیت کیفری در مورد جرائم ارتکابی در فضای سایبری » . پایان نامه حقوق جزا و جرم شناسی،دانشگاه آزاد اسلامی واحد مرکزی تهران

۱۲- زارعی، مصطفی وافروغ،عبدالمحمد،(۱۳۹۳)، بررسی تخصصی جرایم سایبری از منظر علوم حقوق و رایانه، فصلنامه دانش انتظامی دفتر تحقیقات استان بوشهر، سال پنجم، شماره۱۸.

۱۳- زارعی مصطفی (۱۳۹۴)،بررسی نقش رسانه ای شبکه های اجتماعی مجازی با رویکرد مشارکت یاسی و اجتماعی مردم،فصلنامه علمی-تخصصی دانش انتظامی بوشهر،سال ششم،شماره بیستم

۱۴-زندی، محمدرضا،(۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری،تهران، انتشارات جنگل، چاپ اول.

۱۵-سایت خبری فضای مجازی ایران "فیمنا": www.fimna.ir

۱۶-سایت پلیس فضای تولید وتبادل اطلاعات جمهوری اسلامی ایران:www.cyberpolice.ir

۱۷-سایت حقوقی اختبار www.ekhtebar.com

۱۸-سایت تخصصی حقوق ایران www.dad-law.blogfa.com

۱۹-صلاحی ،سهراب ، کشفی، سید مهدی (۱۳۹۵)، جنگ سایبری از منظر حقوق بین الملل با نگاه به دستورالعمل تالین دوفصلنامه علمی پژوهشی مطالعات نرم،دوره ۶، شماره ۱۴، بهار و تابستان

۲۰- صفاری، علی،(۱۳۸۰)، «مبانی نظری پیشگیری وضعی»، مجله تحقیقات حقوقی، شماره ۲۴- ۳۳.

۲۱-عالی پور، حسن(۱۳۹۰)، حقوق کیفری فناوری اطلاعات ،تهران، انتشارات خرسندی ، چاپ نخست.

۲۲-فضلی، مهدی، (۱۳۸۴)،تخریب و اخلال در داده‌ها و سیستم‌های رایانه‌ای، مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات، مرکز مطالعات راهبرداتی و توسعه قضایی قوه قضاییه.
۲۳-فضلی،مهدی(۱۳۸۹)، مسؤولیت کیفری در فضای سایبر، تهران: انتشارات خرسندی، چاپ نخست
۲۴-عالی پور، حسن(۱۳۹۰). « حقوق کیفری فناوری اطلاعات». چاپ نخست،تهران: انتشارات خرسندی.
۲۵-فضلی، مهدی(۱۳۸۹). «مسؤولیت کیفری در فضای سایبر » .چاپ نخست، تهران: انتشارات خرسندی.
۲۶-قانون ایین دادرسی کیفری جدید جمهوری اسلامی ایران-مصوب چهارم اسفند ۱۳۹۲
۲۷-قانون جرایم رایانه ای جمهوری اسلامی ایران. مصوب پنجم خرداد ماه ۱۳۸۸
۲۸-قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان جمهوری اسلامی ایران.مصوب سی و یکم مرداد ماه ۱۳۸۹
۲۹=قانون مجازات جمهوری اسلامی ایران. مصوب یازدهم اردیبهشت ماه ۱۳۹۲
۳۰-کنوانسیون بین المللی جرایم سایبری بوداپست.بیست وسوم نوامبر ۲۰۰۱
۳۱- معتمدنژاد، کاظم، (۱۳۸۳)،وسایل ارتباط جمعی جلد نخست، تهران، انتشارات دانشگاه علامه طباطبایی.
۳۲- نجفی ابرندآبادی، علی حسین، (۱۳۸۳)،پیشگیری عادلانه از جرم، علوم جنایی، مجموعه مقالات در تحلیل از استاد آشوری، انتشارات سمت.
۳۳-نوروزی فیروز، رحمت الله، (۱۳۸۷)، آیین دادرسی کیفری ۲، صلاحیت، تهران، نشر میزان، چاپ اول.
۳۴- نیازپور، امیرحسین،(۱۳۸۳) ،پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم، مجله حقوقی دادگستری، شماره ۴۵.
۳۵-ویلیامز، ماتیو(۱۳۹۱). « بزهکاری مجازی؛ بزه، انحراف و مقرراتگذاری برخط». ترجمه: امیرحسین جلالی فراهانی و محبوبه منفرد، چاپ نخست، تهران : بنیاد حقوقی میزان،

ب) غیرفارسی

36-Adel Azzam Saqf Al Hait, (Vol. 22, 2014.), "Jurisdiction in Cybercrimes: A Comparative Study", Journal of Law, Policy and Globalization,
37-Bruno Simma, and Andreas Mueller, Exercise and the Limits of Jurisdiction,(2011) In:James Crawford, and Martin Koskenniemi (eds), The Cambridge
38-BIAM RAUTD(2012.),etermining the judicial jurisdiction in the Companion to International Law, Cambridge University Press
39- Casey, Eoghan, 2001, Digital Evidence and Computer Crime, Academic Press.
40-Mika, Hayashi , (2013) , Utility of international law of pre internet era
41-Susan W. Brenner1 & Bert-Jaap Koops2 Cite as, (2004) , 4 J. High Tech. L. Approaches to Cybercrime Jurisdiction
42- Sieber,u.1995, Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society.
43- Thomburgh, Dick & s, Lin Herbert, 2004, Editors, Youth, Pornography and The Internet, National Academy Press.
44- T.Kent, Stephen and I. Millett Lynette, 2804, Who goes There? Authentication Through the Lens of Privacy, National Academy Press.
45- United Nations, 2004, Office on Drugs and Crime; the Global Program a gainst Corruption; UN Anti-Corruption Toolkit; Third Edition; Vienna; September.

46- United Nations, 1992, International Review of Criminal Policy-United Nations Manual on the Prevention and Control of Computer - Related Crime, Nos.